Docket No. 218201US2



# IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Koji CHIDA, et al. GAU:

SERIAL NO: NEW APPLICATION EXAMINER:

FILED: HEREWITH

FOR: METHOD, APPARATUS AND PROGRAM FOR QUANTITATIVE COMPETITION AND RECORDING MEDIUM HAVING RECORDED THEREON THE PROGRAM

## REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

| COUNTRY | APPLICATION NUMBER | MONTH/DAY/YEAR |
|---|---|---|
| Japan | 2001-010327 | January 18, 2001 |

Certified copies of the corresponding Convention Application(s)

☒ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

13F0714



# 日　本　国　特　許　庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　１月１８日

出願番号
Application Number: 特願２００１－０１０３２７

出願人
Applicant(s): 日本電信電話株式会社

２００１年１１月３０日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３１０４９４７

【書類名】　特許願

【整理番号】　NTTH126706

【提出日】　平成13年 1月18日

【あて先】　特許庁長官殿

【国際特許分類】　G09C

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　千田　浩司

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　小林　邦生

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　森田　光

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100066153

【弁理士】

【氏名又は名称】　草野　卓

【選任した代理人】

【識別番号】　100100642

【弁理士】

【氏名又は名称】　稲垣　稔

【手数料の表示】

【予納台帳番号】　002897

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9806848

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　大小比較方法、その装置、そのプログラム及びその記録媒体

【特許請求の範囲】

【請求項１】　掲示板装置と、複数のユーザの装置（以下ユーザ装置と記す）と、二つの大小比較装置（以下大小比較装置Ａ、大小比較装置Ｂ、双方の場合は単に大小比較装置と記す）とを備え、

比較の対象となる整数値についてはあらかじめ上限ｍａｘおよび下限ｍｉｎを定めていることを前提とし、全ユーザの意中の値からそれらの最小値およびその最小値を意中の値としたユーザだけが特定できる大小比較方法において、

掲示板装置は、ユーザ装置あるいは大小比較装置より受信した情報を即座に全て公開し、

各ユーザｉ（ｉ＝１，２，…,Ｎ）は、ｍｉｎ以上ｍａｘ以下の意中の値$V_i$を決定してそのユーザ装置へ入力し、ユーザ装置は、ｍｉｎ以上$V_i$未満に対応した情報は等しく、$V_i$以上ｍａｘ以下に対応した情報は異なるような２系列の情報$s_i$および$t_i$を作成し、$s_i$あるいは$t_i$だけでは、$V_i$に関する情報は全く分からないが$s_i$と$t_i$がそろえば$V_i$が分かるものとし、$s_i$を大小比較装置Ａに、$t_i$を大小比較装置Ｂにそれぞれ秘密に送信し、

ｗ以下を意中の値としたユーザがいるかどうかの判定を、大小比較装置Ａは全ユーザの情報$s_i$からｗに対応した情報$s_{i,w}$を取り出し、それらを決められた順序により並べたもの$Seq_{s,w}=s_{1,w}\|s_{2,w}\|\cdots\|s_{N,w}$（‖はデータの連結を表す）を作成し、大小比較装置Ｂは全ユーザの情報$t_i$からｗに対応した情報$t_{i,w}$を取り出し、それらを決められた順序により並べたもの$Seq_{t,w}=t_{1,w}\|t_{2,w}\|\cdots\|t_{N,w}$を作成し、$Seq_{s,w}$と$Seq_{t,w}$を、それ自身の値を明かすことなく比較し、それらが異なっていればｗ以下を意中の値としたユーザがいると判定し、等しければｗ以下を意中の値としたユーザがいないと判定し、その判定に基づき、ｗの値を変更していくことで最小値を決定する、

ことを特徴とする大小比較方法。

【請求項２】　請求項１記載の方法において、

各ユーザｉのユーザ装置は、乱数$R1_i$，$R2_i$を生成し、（$R1_i$，$s_i$）

の組を大小比較装置Ａに、（$R2_i$ ,$t_i$ ）の組を大小比較装置Ｂにそれぞれ秘密に送信し、

また、各組の連結$R1_i \| s_i$ ,$R2_i \| t_i$ についてハッシュ関数ｈによってハッシュ値$H1_i = h(R1_i \| s_i)$ ,$H2_i = (R2_i \| t_i)$ を計算し、それらを掲示板装置に送信し、

掲示板装置は$H1_i$ ,$H2_i$ （ｉ＝１，２，…,Ｎ）を全ユーザのコミットとして公開する

ことを特徴とする大小比較方法。

【請求項３】　請求項２記載の方法において、

大小比較装置は、整数値ｗを共有し、大小比較装置Ａは、$Seq_{s,w}$ についてハッシュ関数ｈによってハッシュ値$HS_w = h(Seq_{s,w})$ を計算し、それを掲示板装置に送信し、

大小比較装置Ｂは、乱数$Seq_{t,w}$ についてハッシュ関数ｈによってハッシュ値$HT_w = h(Seq_{t,w})$ を計算し、それを掲示板装置に送信し、

掲示板装置は、大小比較装置より受信した$HS_w$ ,$HT_w$ を公開して比較し、それらが異なっていればｗ以下を意中の値としたユーザがいると判断し、等しければｗ以下を意中の値としたユーザがいないと判断し、ｗを変更していくことで最小値を決定する

ことを特徴とする大小比較方法。

【請求項４】　請求項３記載の方法において、

大小比較装置は、掲示板装置より予め公開された素数Ｐ（Ｐ－１は大きな素数を約数に持つ）を記憶し、

大小比較装置は、整数値ｗを選択して共有し、

大小比較装置Ａは、乱数$RA_w$ を生成し、連結$RA_w \| HS_w$ についてハッシュ関数ｈによってハッシュ値$HA_w = h(RA_w \| HS_w)$ を計算し、$HS_w^{RAw}$ （ｍｏｄＰ）を計算し、それらの組（$HA_w$ ,$HS_w^{RAw}$ （ｍｏｄＰ））を掲示板装置に送信し、

大小比較装置Ｂは、乱数$RB_w$ を生成し、連結$RB_w \| HT_w$ についてハッシュ関数ｈによってハッシュ値$HB_w = h(RB_w \| HT_w)$ を計算し、$HT_w^{RBw}$

（ｍｏｄＰ）を計算し、それらの組（$HB_w$ ,$HT_w^{RBw}$（ｍｏｄＰ））を掲示板装置に送信し、

次に大小比較装置Ａは、（$HT_w^{RBw}$）$^{RAw}$（ｍｏｄＰ）を、大小比較装置Ｂは、（$HS_w^{RAw}$）$^{RBw}$（ｍｏｄＰ）をそれぞれ計算して、掲示板装置に送信し、

掲示板装置は、大小比較装置より受信した（$HT_w^{RBw}$）$^{RAw}$（ｍｏｄＰ），（$HS_w^{RAw}$）$^{RBw}$（ｍｏｄＰ）を公開して比較し、それらが異なっていればｗ以下を意中の値としたユーザがいると判定し、等しければｗ以下を意中の値としたユーザがいないと判定し、ｗを変更していくことで最小値を決定する

ことを特徴とする大小比較方法。

【請求項５】　請求項３または４記載の方法において、

大小比較装置は、初期値ｗを（ｍａｘ＋ｍｉｎ）／２以下の最大の整数として共有し、ｗ以下を意中の値としたユーザがいると判別されたときはｍａｘにｗを代入し、そうでないときはｍｉｎにｗ＋１を代入して、ｍａｘ＝ｍｉｎ（＝ｍｉｎｖａｌｕｅ）となるまで判別を繰り返し、最小値ｍｉｎｖａｌｕｅを求め、その過程を掲示板装置により逐次公開する

ことを特徴とする大小比較方法。

【請求項６】　請求項３又は５記載の方法において、

最小値ｍｉｎｖａｌｕｅが公開された後、大小比較装置Ａは、$Seq_{s,minvalue}$を、大小比較装置Ｂは、$Seq_{t,minvalue}$を掲示板装置に送信することを特徴とする大小比較方法。

【請求項７】　請求項４又は５記載の方法において、

最小値ｍｉｎｖａｌｕｅが公開された後、大小比較装置Ａは、$Seq_{s,minvalue}$,$RA_{minvalue}$を、大小比較装置Ｂは、$Seq_{t,minvalue}$,$RB_{minvalue}$を掲示板装置に送信することを特徴とする大小比較方法。

【請求項８】　請求項１～７の何れかに記載の方法において、

３以上Ｍ個の大小比較装置$A_j$（ｊ＝１，２，…,Ｍ）が備えられ、

各ユーザｉ（ｉ＝１，２，…,Ｎ）のユーザ装置は$V_i$が入力されるとｍｉｎ以上$V_i$未満に対応した情報は全て等しく、$V_i$以上ｍａｘ以下に対応した情報は全て異なるようなＭ系列の情報$s_{ik}$（ｋ＝１，２，…,Ｍ）を作成し、少なく

ともｓ$_{ik}$のうち２系列ｓ$_{ia}$，ｓ$_{ib}$（ａ≠ｂ）がそろえばＶ$_{i}$が分かるものとし、ｓ$_{ik}$を大小比較装置Ａ$_{k}$にそれぞれ秘密に送信し、

２個の大小比較装置で大小比較を行い、大小比較装置にトラブルが発生すると、他の正常な大小比較装置を用いてその比較動作を継続して行うことを特徴とする大小比較方法。

【請求項９】　請求項１～７の何れかに記載の方法において、

各ユーザｉ（ｉ＝１，２，…，Ｎ）のユーザ装置はＶ$_{i}$が入力されると、ｍｉｎ以上Ｖ$_{i}$以下に対応した情報は異なり、Ｖ$_{i}$＋１以上ｍａｘ以下に対応した情報は等しいような２系列の情報ｓ$_{i}$およびｔ$_{i}$を作成し、ｓ$_{i}$あるいはｔ$_{i}$だけでは、Ｖ$_{i}$に関する情報は全く分からないがｓ$_{i}$とｔ$_{i}$がそろえばＶ$_{i}$が分かるものとし、ｓ$_{i}$を大小比較装置Ａに、ｔ$_{i}$を大小比較装置Ｂにそれぞれ秘密に送信し、上記比較において異なっていればｗ以上を意中の値としたユーザがいると判断し、等しければｗ以上を意中の値としたユーザがいないと判断し、

全ユーザの意中の値からそれらの最大値およびそのユーザだけが特定することを特徴とする大小比較方法。

【請求項１０】　請求項９記載の方法において、

各ユーザｉ（ｉ＝１，２，…，Ｎ）のユーザ装置にＶ$_{i}$が入力されると、ｍｉｎ以上Ｖ$_{i}$以下に対応した情報は異なり、Ｖ$_{i}$＋１以上ｍａｘ以下に対応した情報は等しいような２系列の情報ｓ$_{i}$およびｔ$_{i}$として、一方向性関数Ｆに対して$F^{d}$（ｓ$_{i}$）＝$F^{d}$（ｔ$_{i}$）（ｄ＝０，１，…，Ｖ$_{i}$－ｍｉｎ）かつ$F^{e}$（ｓ$_{i}$）≠$F^{e}$（ｔ$_{i}$）（ｅ＝Ｖ$_{i}$－ｍｉｎ＋１，…，ｍａｘ－ｍｉｎ）を生成する（ここで例えば$F^{3}$（ｓ$_{i}$）はＦ（Ｆ（Ｆ（ｓ$_{i}$））を表す）ことを特徴とする大小比較方法。

【請求項１１】　請求項１～７の何れかに記載の方法において、

各ユーザｉ（ｉ＝１，２，…，Ｎ）のユーザ装置はＶ$_{i}$が入力されると、ｍｉｎ以上Ｖ$_{i}$未満に対応した情報は等しく、Ｖ$_{i}$以上ｍａｘ以下に対応した情報は異なるような２系列の情報ｓ$_{i}$およびｔ$_{i}$として一方向性関数Ｆに対して、$F^{d}$（ｓ$_{i}$）≠$F^{d}$（ｔ$_{i}$）（ｄ＝０，１，…，ｍａｘ－Ｖ$_{i}$）かつ$F^{e}$（ｓ$_{i}$）＝$F^{e}$（ｔ$_{i}$）（ｅ＝ｍａｘ－Ｖ$_{i}$＋１，…，ｍａｘ－ｍｉｎ）を生成する（ここで例えば$F^{3}$（ｓ）でＦ（Ｆ（Ｆ（ｓ））を表す）

ことを特徴とする大小比較方法。

【請求項１２】　大小比較方法に用いられるユーザ装置であって、

比較の対象となる整数値についての上限ｍａｘおよび下限ｍｉｎが記憶された記憶部と、

ｍｉｎ以上ｍａｘ以下の意中の値$V_i$を入力する入力手段と、

$V_i$とｍｉｎ，ｍａｘが入力され、ｍｉｎ以上$V_i$未満に対応した情報は等しく、$V_i$以上ｍａｘ以下に対応した情報は異なる２系列の情報$s_i$および$t_i$、ｍｉｎ以上$V_i$以下に対応した情報は異なり、$V_i$＋１以上ｍａｘ以下に対応した情報は等しいような２系列の情報$s_i$および$t_i$の一方を生成して出力する２系列生成部と、

$s_i$および$t_i$が入力され、これらに対する一方向性関数を演算して演算結果$H1_i$，$H2_i$を出力する一方向性関数演算部と、

$s_i$を大小比較装置Ａへ、$t_i$を大小比較装置Ｂへ、$H1_i$および$H2_i$を掲示板装置へそれぞれ送信する送信部と

を具備するユーザ装置。

【請求項１３】　大小比較方法に用いられる大小比較装置であって、

各ユーザ装置から送られた、比較の対象となる整数値についての上限ｍａｘから下限ｍｉｎまでの数よりなる系列を受信し、掲示板装置から送られた整数値ｗを受信する受信部と、

受信した系列を記憶する記憶部と、

各ユーザの系列中から受信したｗ番目の情報を入力して、これらの連結に対して一方向性関数を演算し、その演算結果を出力する一方向性関数演算部と、

上記一方向性関数演算結果を上記掲示板装置へ送信する送信部と

を具備する大小比較装置。

【請求項１４】　大小比較方法に用いられるユーザ装置のコンピュータを、

比較の対象となる整数値についての上限ｍａｘ以下、下限ｍｉｎ以上の意中の値$V_i$を入力する入力手段、

ｍｉｎ以上$V_i$未満に対応した情報は等しく、$V_i$以上ｍａｘ以下に対応した情報は異なる２系列の情報$s_i$および$t_i$、ｍｉｎ以上$V_i$以下に対応した情報

は異なり、$V_i$ ＋１以上ｍａｘ以下に対応した情報は等しいような２系列の情報 $s_i$ および $t_i$ の一方を生成する手段、

$s_i$ および $t_i$ に対しそれぞれ一方向性関数を演算して演算結果 $H1_i$，$H2_i$ を出力する手段、

$s_i$ を大小比較装置Ａへ、$t_i$ を大小比較装置Ｂへ、$H1_i$ および $H2_i$ を掲示板装置へそれぞれ送信する手段、

として機能させるためのプログラム。

【請求項１５】　大小比較方法に用いられるユーザ装置のコンピュータを、

比較の対象となる整数値についての上限ｍａｘ以下、下限ｍｉｎ以上の意中の値 $V_i$ を入力する入力手段、

ｍｉｎ以上 $V_i$ 未満に対応した情報は等しく、$V_i$ 以上ｍａｘ以下に対応した情報は異なる２系列の情報 $s_i$ および $t_i$、ｍｉｎ以上 $V_i$ 以下に対応した情報は異なり、$V_i$ ＋１以上ｍａｘ以下に対応した情報は等しいような２系列の情報 $s_i$ および $t_i$ の一方を生成する手段、

$s_i$ および $t_i$ に対しそれぞれ一方向性関数を演算して演算結果 $H1_i$，$H2_i$ を出力する手段、

$s_i$ を大小比較装置Ａへ、$t_i$ を大小比較装置Ｂへ、$H1_i$ および $H2_i$ を掲示板装置へそれぞれ送信する手段、

として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、情報セキュリティ技術の応用技術であって、例えばインターネットなどによるオンライン上で、複数のユーザ（利用者）が意中の値を秘密に保持したまま比較し、最大値あるいは最小値と、それを意中の値としたユーザだけが特定される方法およびその装置に関するものである。

【０００２】

【従来の技術】

大小比較がオンラインで実施される例として「電子入札方式」などがある。上記方式では、最大値あるいは最小値と、それを意中の値としたユーザは特定されるが、その他の情報は秘密に保持される技術が例えば

・小林，森田，「大小比較に一方向性関数を用いた効率的な入札方式」，ＩＳＥＣ９９，などに示されている。また、

・H.Kikuchi,M.Harkavy,D.Tygar, "Multi-round anonymous auction protocols" In IEEE Workshop on Dependable and Real-Time E-Commerce System,1998,

では、ある数値に対してそれ以上あるいはそれ以下を意中の値としたユーザがいるかどうかだけが分かる方式を提案している。しかしながら最大値あるいは最小値を意中の値としたユーザが複数いる場合にそのユーザを特定できないことと、最大値あるいは最小値を意中の値としたユーザが２番目の数値を知り得てしまうという問題点があった。

【０００３】

【発明が解決しようとする課題】

この発明の目的は複数のユーザが意中のものとした値の大小をオンラインで比較して、安全かつ高速に、これらの最大値あるいは最小値、更に必要に応じてそれを意中の値としたユーザだけが特定され、他は秘密が保持されるための方法およびその装置を提供することにある。

【０００４】

【課題を解決するための手段】

比較の対象となる整数値についてはあらかじめ上限ｍａｘおよび下限ｍｉｎを定めておく。なお、最大値、最小値のどちらを特定するかには本質的に変わりはないので、ここでは最小値を特定する場合のみを説明する。

各ユーザｉ（ｉ＝１，２，…，Ｎ）は、ｍｉｎ以上ｍａｘ以下の意中の値$V_i$を決定した後、ユーザ装置により、ｍｉｎ以上$V_i$未満に対応した情報は等しく、$V_i$以上ｍａｘ以下に対応した情報は異なるような２系列の情報$s_i$および$t_i$を作成し、$s_i$を大小比較装置Ａに、$t_i$を大小比較装置Ｂにそれぞれ秘密に送信する。$s_i$あるいは$t_i$だけでは、$V_i$に関する情報は全く分からないために、誰にもまた各大小比較装置にさえも$V_i$が知られることはない。

【０００５】

全ユーザの意中の値に関する情報$s_i$，$t_i$（ｉ＝１，２，…，Ｎ）がそろったら次に最小値を決定する。この手順は自由であるが、効率的な手法を以下に示す。まず（ｍａｘ＋ｍｉｎ）／２以下の最大の整数（これをｗとする）以下を意中の値としたユーザがいるかどうかの判定を、大小比較装置Ａは全ユーザの情報$s_i$からｗに対応した情報$s_{i,w}$を取り出し、それらを決められた順序（例えばユーザに予め番号が割り振られていてその番号順など）により並べたものＳｅｑ$_{s,w}$＝$s_{1,w}\|s_{2,w}\|\cdots s_{N,w}$（‖はデータの連結を表す）を作成し、大小比較装置Ｂは全ユーザの情報$t_i$からｗに対応した情報$t_{i,w}$を取り出し、それらを決められた順序により並べたものＳｅｑ$_{t,w}$＝$t_{1,w}\|t_{2,w}\|\cdots t_{N,w}$を作成し、Ｓｅｑ$_{s,w}$とＳｅｑ$_{t,w}$を、一方向性関数や暗号関数などを用いてそれ自身の値を明かすことなく比較し、それらが異なっていればｗ以下を意中の値としたユーザがいると判定し、ｍａｘにｗを代入し、同様にＳｅｑ$_{s,w}$、Ｓｅｑ$_{t,w}$を生成し、前記比較を行い等しければｗ以下を意中の値としたユーザがいないと判定し、ｍｉｎにｗ＋１を代入して、上記操作をｍｉｎ＝ｍａｘ（＝ｍｉｎｖａｌｕｅ）となるまで繰り返すことで最小値ｍｉｎｖａｌｕｅを決定する。

【０００６】

最後にＳｅｑ$_{s,minvalue}$，Ｓｅｑ$_{t,minvalue}$を公開して、誰もが最小値ｍｉｎｖａｌｕｅを意中の値としたユーザを特定することができるようにする。

【０００７】

【発明の実施の形態】

大小比較を行う際、上限の整数値ｍａｘ、下限の整数値ｍｉｎ、大きな素数Ｐ（Ｐ－１は大きな素因子を約数に持つ、つまり離散対数問題をより所とする暗号方式の条件を満すようにし）がすでに決められているものとする。

まず第１の実施形態として、２つの大小比較装置を用いて全ユーザの意中の値から最小値およびそれを意中の値としたユーザのみが特定できる方法を示す。次に第２の実施形態として、３つの大小比較装置を用いるが、そのうちの一つは大小比較の途中でシステムがダウンした場合に、全ユーザのだした意中の値から最小値およびそれを意中の値としたユーザのみを特定できる方法を示す。

第１の実施形態

まずはじめに、第１の実施形態における全体の位置付けを図１に示す。大小比較装置１５Ａ及び１５Ｂ、掲示板装置１９が設けられ、各ユーザ装置１３－１～１３－Ｎは図に示していない通信網を通じて大小比較装置１５Ａ及び１５Ｂ、また掲示板装置１９と通信することができ、大小比較装置１５Ａ及び１５Ｂは掲示板装置１９と通信することができる。

【０００８】

なお番号１６は掲示板装置２１に対する閲覧情報を示す。また掲示板装置２１にはデータベース２３が接続されている。

ユーザｉ（ｉ＝１，２，…，Ｎ）は、ｍｉｎ以上ｍａｘ以下の意中の整数値$V_i$を定め、そのユーザ装置１３－ｉはキーボードなどの入力手段３０により入力する。ユーザ装置１３－ｉの２系列生成部３３は入力された$V_i$にもとづき２系列の情報$s_i$と$t_i$とを生成する。$s_i=\{s_{i,1}, s_{i,2}, \cdots, s_{i,M}\}$，$t_i=\{t_{i,1}, t_{i,2}, \cdots, t_{i,M}\}$、Ｍはｍｉｎからｍａｘまでのユーザが意中の値とすることができる値の数であり、ここで$V_i$がｍｉｎからｖ番目とすると、$s_{i,1}=t_{i,1}$，$s_{i,2}=t_{i,2}$，…，$s_{i,v-1}=t_{i,v-1}$，$s_{i,v}\neq t_{i,v}$，$s_{i,v+1}\neq t_{i,v+1}$，…，$s_{i,M}\neq t_{i,M}$とする。つまり$s_i$と$t_i$はｍｉｎ以上$V_i$未満の対応した要素（情報）は互いに等しく、$V_i$以上ｍａｘ以下の対応した要素は互いに異なる。これらは例えば図６に示すように予め決めたビット数からなる乱数を$V_i$－ｍｉｎ＝ｖ－１個、$a_1$，$a_2$，…，$a_{(v-1)}$を生成し（Ｓ１）、ｎをｖとし（Ｓ２）、２個の乱数を生成し（Ｓ３）、この２個の乱数が等しくなければ（Ｓ４）、ｎを＋１し（Ｓ５）、ｎがｍａｘ以上でなければステップＳ３に戻り（Ｓ６）、ステップＳ４で２つの乱数が等しければステップＳ３に戻り、ステップＳ６でｎがｍａｘ以上であればステップＳ７に移り、$a_1$，…，$a_{(v-1)}$を$s_{i1}$，$s_{i2}$，…，$s_{i(v-1)}$と$t_{i,1}$，$t_{i,2}$，…，$t_{i,(v-1)}$とにし、これらに対し各２個ずつ発生した乱数を１個ずつ順次振分けて、残りの$s_{i,v}$，…，$s_{i,M}$と$t_{i,v}$，…$t_{i,M}$とする。

【０００９】

乱数生成部３１から乱数$R1_i$，$R2_i$を生成し、（$s_i$，$R1_i$）の組を大小比

較装置１５Ａに、（$t_i$，Ｒ$2_i$）の組を大小比較装置１５Ｂにそれぞれ秘密に、例えば暗号化部３４で暗号化して送信する（この暗号化関数をＤとする）。また、ハッシュ関数演算部３５で各組の連結$s_i \| R1_i$，$t_i \| R2_i$についてハッシュ関数ｈによってハッシュ値$H1_i = h(s_i \| R1_i)$，$H2_i = h(t_i \| R2_i)$を計算し、それらを掲示板装置１９に送信する。なお、ｍａｘ、ｍｉｎ２系列$s_i$，$t_i$、乱数Ｒ$1_i$，Ｒ$2_i$，$V_i$は記憶部３２に記憶され、各情報の大小比較装置１５Ａ，１５Ｂや掲示板装置１９への送信は送信部３６が行う。記憶部３２に対する読み書き、各部に対する動作指示は制御部３７により行う。このユーザ装置１３－ｉはコンピュータによりプログラムを実行させて機能させるように構成してもよい。

【００１０】

各ユーザｉはハッシュ値Ｈ$1_i$およびＨ$2_i$を掲示板装置１９に送信し、その値が公開されることで$V_i$をコミットしたことになる。つまり$V_i$を明かすことなく、$V_i$を意中の値としたことを登録したことになる。これにより、以降意中の値を変更不可能とするとともに、もしなんらかの理由で自分の意中の値より大きい値が最小値となったときは、$s_i$，Ｒ$1_i$，$t_i$，Ｒ$2_i$を公開することで自分の意中の値が最小値であることを示すことができる。また、乱数Ｒ$1_i$，Ｒ$2_i$を連結させているのは、$H1_i = h(s_i)$，$H2_i = h(t_i)$とすると$s_i$あるいは$t_i$を知っているともう一方の値もあたりがつけやすくなるケースにも対応するため（$s_i$，$t_i$を知れば$V_i$が分かる）、大小比較装置１５Ａ，１５Ｂに対しても秘密を高めるためであり、乱数Ｒ$1_i$，Ｒ$2_i$を省略してもよい。

【００１１】

大小比較装置１５Ａ，１５Ｂは図３、図４に示すように受信部４０に受信された各ユーザ装置１３－１～１３－Ｎからの情報系列$s_1$～$s_N$，$t_1$～$t_N$はそれぞれ記憶部４１に格納され、また受信した乱数Ｒ$1_1$～Ｒ$1_N$，Ｒ$2_1$～Ｒ$2_N$も格納される。記憶部４１には前述した大きな素数Ｐも格納されてある。

全てのユーザ装置１３－１～１３－Ｎから情報系列$s_i$，$t_i$、乱数Ｒ$1_i$，Ｒ$2_i$、ハッシュ値Ｈ$1_i$，Ｈ$2_i$が送信されると、例えば掲示板装置１９から、（ｍａｘ＋ｍｉｎ）／２以下の最大の整数を初期値ｗとして大小比較装置１５Ａ，

１５Ｂに送信され、ｗが大小比較装置１５Ａ，１５Ｂの受信部４０に受信されると、大小比較装置１５Ａは、図３に示すように乱数生成部４２から乱数$RA_w$を生成し、全ユーザ装置から受信した$s_i$のｗに対応した情報$s_{i,w}$を記憶部４１から取り出しそれらをユーザ１，ユーザ２，…，ユーザＮの順に並べたもの$Seq_{s,w}=s_{1,w}\|s_{2,w}\|\cdots\|s_{N,w}$を作成し、ハッシュ関数演算部４３でハッシュ関数ｈによって$Seq_{s,w}$に対するハッシュ値$HS_w=h(Seq_{s,w})$および$RA_w\|HS_w$に対するハッシュ値$HA_w=h(RA_w\|HS_w)$を計算し、その$HS_w$と乱数$RA_w$をべき乗剰余演算部４４に入力して$HS_w^{RAw}(mod P)$を計算し、それら（$HA_w$，$HS_w^{RAw}(mod P)$）の組を掲示板装置１９に送信部４５より送信する。

【００１２】

大小比較装置１５Ｂは図４に示すように乱数生成部４２、乱数$RB_w$を生成し、全ユーザ装置から受信した$t_i$のｗに対応した情報$t_{i,w}$を記憶部４１から取り出し、それらをユーザ１，ユーザ２，…，ユーザＮの順に並べたもの$Seq_{t,w}=t_{1,w}\|t_{2,w}\|\cdots\|t_{N,w}$を作成し、ハッシュ関数演算部４３に入力してハッシュ関数ｈによって$Seq_{t,w}$に対するハッシュ値$HT_w=h(Seq_{t,w})$および$RB_w\|HT_w$に対するハッシュ値$HB_w=h(RB_w\|HT_w)$を計算し、$HT_w$と$RB_w$をべき乗剰余演算部４４に入力して$HT_w^{RBw}(mod P)$を計算し、それら（$HB_w$，$HT_w^{RBw}(mod P)$）の組を掲示板装置１９に送信部４５により送信する。

【００１３】

次に大小比較装置１５Ａは、掲示板装置１９より公開された$HT_w^{RBw}(mod P)$をべき乗剰余演算部４４に閲覧入力して、$(HT_w^{RBw})^{RAw}(mod P)$を計算し、その計算結果を掲示板装置１９に送信する。大小比較装置１５Ｂも同様に、掲示板装置１９より公開された$HS_w^{RAw}(mod P)$をべき乗剰余演算部４４に閲覧入力して$(HS_w^{RAw})^{RBw}(mod P)$を計算し、その結果を掲示板装置１９に送信する。

$HS_w$と$HT_w$が等しければ、掲示板装置１９に送信された$(HT_w^{RBw})^{RAw}(mod P)$と$(HS_w^{RAw})^{RBw}(mod P)$は等しく、またＰが大きな素数であ

り、かつＰ－１は大きな素因子を約数にもつから、$HS_w$と$HT_w$が異なり（$HT_w^{RBw})^{RAw}$（ｍｏｄＰ）と（$HS_w^{RAw})^{RBw}$（ｍｏｄＰ）が等しくなる可能性は無視できるほど小さいことから、（$HT_w^{RBw})^{RAw}$（ｍｏｄＰ）と（$HS_w^{RAw})^{RBw}$（ｍｏｄＰ）が等しければ$s_{1,w}=t_{1,w}$，$s_{2,w}=t_{2,w}$，…，$s_{N,w}=t_{N,w}$であるから、ｗ＋１以上が最小値ということになり、異なればｗ以下が最小値ということが圧倒的確率で分かる。掲示板装置１９はこのことを判定し、もし等しければｍｉｎにｗ＋１を代入し、異なればｍａｘにｗを代入して上記操作を繰り返す。以上のことを繰り返すことにより、およそｌｏｇ（ｍａｘ－ｍｉｎ）回でｍａｘ＝ｍｉｎ（＝ｍｉｎｖａｌｕｅ）となる。このｍｉｎｖａｌｕｅが最小値となる。この過程を図５に示す。つまりまず（ｍａｘ＋ｍｉｎ）／２以下の最大の整数をｗとしてそのｗについて図３、図４を参照して説明したように、大小比較装置１５Ａ、１５Ｂで$HA_w$，$HS_w^{RAw}$ｍｏｄＰ，$HB_w$，$HT_w^{RBw}$ｍｏｄＰをそれぞれ求め、更に（$HT_w^{RBw})^{RAw}$ｍｏｄＰ，（$HS_w^{RAw})^{RBw}$ｍｏｄＰをそれぞれ計算し（ｓ１）、この計算結果が一致しているかを調べ（ｓ２）、一致していればｗ＋１をｍｉｎとし（ｓ３）、ｍａｘ＝ｍｉｎになったかを調べ（ｓ４）、なっていなければステップｓ１に戻り、ステップｓ２で一致していなければ、ｗをｍａｘとしてステップｓ４に移る（ｓ５）。ステップｓ４でｍａｘとｍｉｎとが等しければ、そのｍｉｎを最小値（ｍｉｎｖａｌｕｅ）、つまりユーザ１１－１～１１－Ｎがそれぞれ意中の値$V_1$～$V_N$として、コミットしたもののうちの最小値が求まったことになる。

【００１４】

この最小値ｍｉｎｖａｌｕｅが分かった後、大小比較装置１５Ａ，１５Ｂはその最小値と対応する、$Seq_{s,minvalue}$，$RA_{minvalue}$，$Seq_{t,minvalue}$，$RB_{minvalue}$を掲示板装置１９に送信することにより、全ユーザ１１－１～１１－Ｎは、それら２系列に対して対応する部分$s_{j,w}\neq t_{j,w}$と異なる情報が入ったｊ番目の部分に該当するユーザが最小値を意中の値としたと特定できる。$Seq_{s,w}$，$Seq_{t,w}$の配列順が知られていれば、前記異なるｊ番目に該当するユーザｊが意中のものとした値$V_j$が最小値であることを特定できる。

【００１５】

最後に不正がなかったことを確認するため、大小比較装置１５Ａ，１５Ｂは最小値を意中の値としたユーザｊのＲ１$_j$，ｓ$_j$，Ｒ２$_j$，ｔ$_j$を掲示板装置１９に送信する。全ユーザは掲示板装置１９より公開されたコミットとの対応を確認することができる。つまり、Ｒ１$_j$，ｓ$_j$，Ｒ２$_j$，ｔ$_j$の公開によりユーザｊは自身が意中の値としたものが最小となったことを知ることができ、また全てのユーザは、そのユーザ装置により、ｈ（ｓ$_j$‖Ｒ１$_j$）及びｈ（ｔ$_j$‖Ｒ２$_j$）を演算し、これらがユーザｊがコミットしたＨ１$_j$及びＨ２$_j$とそれぞれ一致することを確認して、正しい操作（大小比較）が行われたことを知ることができる。なおＳｅｑ$_{s,w}$、Ｓｅｑ$_{t,w}$の配列順とユーザとの関係が公開されていない場合には、Ｒ１$_j$，ｓ$_j$，Ｒ２$_j$，ｔ$_j$を公開した時点で、最小値を意中の値としたユーザｊが特定される。

【００１６】

なお仮にＨＴ$_w$を知ったものがＨＳ$_w$を推定でき、それが正しければ他のユーザの意中の値を知ることができるが、Ｐが大きな素数であり、かつＰ－１は大きな素因子を約数にもつようにされているためＨＳ$_w^{RAw}$のＲＡ$_w$を求めることが困難であるため、そのＨＳ$_w$が真に正しいものか知ることができない。従って他のユーザが意中の値を知ることはできない。

また大小比較装置１５Ａ，１５Ｂにおいて乱数ＲＡ$_w$，ＲＢ$_w$を省略してもよいが、ＲＡ$_w$，ＲＢ$_w$を用い、最後に、ＲＡ$_{minvalue}$，ＲＢ$_{minvalue}$を公開することにより、これらとＳｅｑ$_{s,minvalue}$，Ｓｅｑ$_{t,minvalue}$を用いることにより、大小比較処理が正しく行われたかを確認することができる。

【００１７】

大小比較装置１５Ａ，１５Ｂにおいてはその記憶部４１に対する読み書き、受信情報の処理、各送信情報を対応する装置へ送信部４５により送信させ、その他の各部の動作をさせることなどを制御部４６で行う。この大小比較装置１５Ａ，１５Ｂもコンピュータによりプログラムを実行させて機能させることもできる。

掲示板装置１９はその機能構成を特に図に示さなかったが、各ユーザ装置、大小比較装置１５Ａ，１５Ｂとの送受信部を備え、受信された情報をデータベース２３に格納し、閲覧要求があれば、対応する情報をデータベース２３が読み出し

て、要求元へ送信し、また図５に示した処理とその実行に必要な送受信を行う。この掲示板装置１９もコンピュータによりプログラムを実行させて機能させるようにすることもできる。

第２の実施形態

ユーザｉ（ｉ＝１，２，…，Ｎ）は、ｍｉｎ以上ｍａｘ以下の意中の整数値$V_i$を定め、ユーザ装置によりｍｉｎ以上$V_i$未満に対応した情報は全て等しく、$V_i$以上ｍａｘ以下に対応した情報は全て異なるような３系列の情報$s_i$，$t_i$，$u_i$を作成し、乱数$R1_i$，$R2_i$，$R3_i$を生成し、（$s_i$，$R1_i$）の組を大小比較装置Ａに、（$t_i$，$R2_i$）の組を大小比較装置Ｂに（$u_i$，$R3_i$）の組を大小比較装置Ｃに、それぞれ秘密に送信する。また、各組の連結$s_i \| R1_i$，$t_i \| R2_i$，$u_i \| R3_i$についてハッシュ関数ｈによってハッシュ値$H1_i = h(s_i \| R1_i)$，$H2_i = h(t_i \| R2_i)$，$H3_i = h(u_i \| R3_i)$を計算し、それらを掲示板装置１９に送信する。

【００１８】

各ユーザｉは$H1_i$および$H2_i$および$H3_i$を掲示板装置に送信し、その値が公開されることで$V_i$をコミットしたことになる。これにより、以降意中の値を変更不可能とするとともに、もしなんらかの理由で自分の意中の値より大きい値が最小値となったときは、（$s_i$，$R1_i$），（$t_i$，$R2_i$），（$u_i$，$R3_i$）の少なくとも２組を公開することで自分の意中の値が最小値であることを示すことができる。

以降、大小比較装置は２つで充分であるから、その２つを大小比較装置ＡおよびＢとする。

【００１９】

前述と同様に大小比較装置は、まず初期値ｗを（ｍａｘ＋ｍｉｎ）／２以下の最大の整数とし、大小比較装置Ａは、乱数$RA_w$を生成し、全ユーザ装置から受信した$s_i$のｗに対応した情報$s_{i,w}$を取り出し、それらをユーザ１，ユーザ２，…，ユーザＮの順に並べたもの$Seq_{s,w} = s_{1,w} \| s_{2,w} \| \cdots \| s_{N,w}$を作成し、ハッシュ関数ｈによってハッシュ値$HS_w = h(Seq_{s,w})$および$HA_w = h(RA_w \| HS_w)$および$HS_w^{RAw} (mod P)$を計算し、それら（$HA_w$

，$HS_w^{RAw}$（ｍｏｄＰ））の組を掲示板装置に送信する。大小比較装置Ｂは、乱数$RB_w$を生成し、全ユーザ装置から受信した$t_i$のｗに対応した情報$t_{i,w}$を取り出し、それらをユーザ１，ユーザ２，…，ユーザＮの順に並べたもの$Seq_{t,w}=t_{1,w}\|t_{2,w}\|\cdots\|t_{N,w}$を作成し、ハッシュ関数ｈによってハッシュ値$HT_w=h(Seq_{t,w})$および$HB_w=h(RB_w\|HT_w)$および$HT_w^{RBw}$（ｍｏｄＰ）を計算し、それら（$HB_w$，$HT_w^{RBw}$（ｍｏｄＰ））の組を掲示板装置に送信する。

【００２０】

次に大小比較装置Ａは、掲示板装置より公開された$HT_w^{RBw}$（ｍｏｄＰ）を用いて、$(HT_w^{RBw})^{RAw}$(ｍｏｄＰ）を計算し、それを掲示板装置に送信し、大小比較装置Ｂは、掲示板装置より公開された$HS_w^{RAw}$(ｍｏｄＰ）を用いて、$(HS_w^{RAw})^{RBw}$(ｍｏｄＰ）を計算し、それを掲示板装置に送信する。

$HS_w$と$HT_w$が等しければ$(HT_w^{RBw})^{RAw}$(ｍｏｄＰ）と$(HS_w^{RAw})^{RBw}$(ｍｏｄＰ）は等しく、またＰが大きな素数であり、かつＰ－１は大きな素因子を約数にもつから、$HS_w$と$HT_w$が異なり$(HT_w^{RBw})^{RAw}$(ｍｏｄＰ）と$(HS_w^{RAw})^{RBw}$(ｍｏｄＰ）が等しくなる可能性は無視できるほど小さいことから、$(HT_w^{RBw})^{RAw}$(ｍｏｄＰ）と$(HS_w^{RAw})^{RBw}$(ｍｏｄＰ）が等しければｗ＋１以上が最小値ということになり、異なればｗ以下が最小値ということが圧倒的確率で分かる。もし等しければｍｉｎにｗ＋１を代入し、異なればｍａｘにｗを代入して上記操作を繰り返すことにより、およそlog(ｍａｘ－ｍｉｎ)回でｍａｘ＝ｍｉｎ（＝ｍｉｎｖａｌｕｅ）となる。このｍｉｎｖａｌｕｅが最小値となる。

【００２１】

最小値ｍｉｎｖａｌｕｅが分かった後、大小比較装置は、$Seq_{s,minvalue}$，$RA_{minvalue}$，$Seq_{t,minvalue}$，$RB_{minvalue}$を掲示板装置に送信することで、全ユーザは、それら２系列に対して異なる情報が入った部分に該当するユーザが最小値を意中の値としたユーザｊであるということを特定できる。

上記過程で、トラブルにより一方の大小比較装置、例えばＢのシステムがダウンしたとする。しかし、大小比較装置Ｂのもつ情報と大小比較装置Ｃのもつ情報は本質的に同じであるから、そのまま大小比較装置Ｂの操作を大小比較装置Ｃが

引き継ぐことができる。

【００２２】

最後に不正がなかったことを確認するため、大小比較装置は最小値を意中の値としたユーザｊのＲ１$_j$，ｓ$_j$，Ｒ３$_j$，ｕ$_j$を掲示板装置に送信することで、全ユーザは掲示板装置より公開されたコミットとの対応を確認することができる。このように大小比較装置を更に多く設け、それに応じて情報系列の数を増加して同様に処理することにより、大小比較装置がトラブルになりシステムダウンした場合の安全性を高くすることもできる。

上述したことから理解できるように、各大小比較装置１５Ａ，１５Ｂは各ユーザ装置から受信した情報が正しいものであるかを掲示板装置１９の対応公開情報Ｈ１$_i$，Ｈ２$_i$により検証することができる。また大小比較装置１５Ａ，１５Ｂの両者でＲ１$_i$，ｓ$_i$，Ｒ２$_i$，ｔ$_i$を公開することにより、ユーザｉの意中の値Ｖ$_i$が確かなものであることを検証することができる。

【００２３】

大小比較装置１５Ａ，１５ＢはＳｅｑ$_{s,minvalue}$，Ｓｅｑ$_{t,minvalue}$を掲示板装置１９に送信して公開した後、必要に応じてＳｅｑ$_{s,z}$，Ｓｅｑ$_{t,z}$（ｚ＝ｍｉｎ，ｍｉｎ＋１，…，ｍｉｎｖａｌｕｅ）のうち大小比較処理に用いられたものを掲示板装置１９へ送信し、ｍｉｎｖａｌｕｅが正しいものであることを明らかにしてもよい。

上述においては大小比較装置１５Ａ，１５Ｂで作成したＳｅｑ$_{s,w}$，Ｓｅｑ$_{t,w}$をそれ自身の値を明かすことなく、比較するために一方向性関数を用いたが、例えば同一の暗号鍵で、同一の暗号演算をＳｅｑ$_{s,w}$，Ｓｅｑ$_{t,w}$に対して、その結果を掲示板装置１９へ送信して比較を行ってもよい。

【００２４】

この発明では、要は、大小比較装置１５Ａ，１５Ｂにおいて、ｗに対応した情報ｓ$_{i,w}$，ｔ$_{i,w}$をそれぞれ取出し、それらを決められた順序に並べたものＳｅｑ$_{s,w}$とＳｅｑ$_{t,w}$を作り、これらを明すことなく比較して、異なるか等しいかにより、ｗ以下（最大値を求める場合はｗ以上）に意中の値としたユーザがいるかを判定し、その判定結果にもとづき、ｗを変更すればよい。ＨＳ$_w$とＨＴ$_w$とを比較

して、上記判定をしてもよい。乱数Ｒ１$_i$，Ｒ２$_i$は安全性を高めたのであり、必ずしも用いなくてもよい。従ってＨ１$_i$＝ｈ（ｓ$_i$），Ｈ２$_i$＝ｈ（ｔ$_i$）として掲示板装置へ送信してもよい。

【００２５】

２系列情報ｓ$_i$，ｔ$_i$としては例えば最小値を求める場合は一方向性関数Ｆに対して、$F^d(s_i) \neq F^d(t_i)$、（ｄ＝０，１，…，ｍａｘ－Ｖ$_i$）かつ$F^e(s_i) = F^e(t_i)$、（ｅ＝ｍａｘ－Ｖ$_i$＋１，…，ｍａｘ－ｍｉｎ）となるようなものにしてもよい。ここで例えば$F^3(s_i)$はＦ（Ｆ（Ｆ（ｓ$_i$））を表わす。情報系列ｓ$_i$は

$s_i = \{s_{i1} = F^{max-min}(s_i),\ s_{i2} = F^{max-min-1}(s_i),\ \cdots,\ F^{max-vi+1}(s_i),\ F^{max-Vi}(s_i),\ \cdots,\ s_{i,M-1} = F(s_i),\ s_{iM} = s_i\}$

となる。つまり情報系列の順番が小さい方が最も多く関数演算される。最大値を求める場合も同様にこのように求めてもよい。このように関数値を用いるとｍａｘ－ｍｉｎの数が多くなっても各系列の１つの情報のビット数は一定であるが、乱数を用いる場合は、用いる乱数のビット数を多くする必要があり、伝送や処理が大変になる。

【００２６】

上述においては各ユーザの意中の値Ｖ$_i$の最小値を決定したが、最大値の決定も同様に行うことができる。この場合は２系列情報ｓ$_i$とｔ$_i$としては、ｍｉｎ以上Ｖ$_i$以下に対応した情報はｓ$_i$とｔ$_i$とで異なり、Ｖ$_i$＋１以上ｍａｘ以下に対応した情報はｓ$_i$とｔ$_i$とで等しいようにする。また各選択されたｗについてのＳｅｑ$_{s,w}$とＳｅｑ$_{t,w}$の比較、ＨＳ$_w$＝ｈ（Ｓｅｑ$_{s,w}$）とＨＴ$_w$＝ｈ（Ｓｅｑ$_{t,w}$）の比較、$(HT_w^{RBw})^{RAw}$ｍｏｄＰと$(HS_w^{RAw})^{RBw}$ｍｏｄＰの比較において異なっていればｗ以上を意中の値としたユーザがいると判断し、等しければｗ以上を意中の値としたユーザがいないと判断し、等しい場合はｗをｍａｘとし異なっていれば、ｗ＋１をｍｉｎとして、同様の処理を繰り返せばよい。

【００２７】

ｗの決定は先に述べたようにすると効率的に最小値又は最大値を求めることができるが、ｗを例えばｍｉｎ又はｍａｘから順次変化させて大小比較を行っても

よい。更に１つの大小比較装置が最初のｗを決定し、ｗを掲示板装置１９を介して他の大小比較装置へ送り、掲示板装置１９から必要な情報を受け取って、図５に示した処理を行ってもよい。

【００２８】

【発明の効果】

以上述べたようにこの発明によれば、ユーザは意中の値に関する情報を１回だけ各大小比較装置および掲示板装置に送信するだけで、高速に最大値あるいは最小値とを特定でき、必要に応じてそれを意中の値としたユーザのみが特定できる、秘匿性の高い大小比較が実現できる。

【図面の簡単な説明】

【図１】

第１の実施形態の全体のシステム構成例を示す図。

【図２】

ユーザ装置のおもな機能構成例を示す図。

【図３】

大小比較装置１５Ａのおもな機能構成例を示す図。

【図４】

大小比較装置１５Ｂのおもな機能構成例を示す図。

【図５】

最小値を特定するための流れ図。

【図６】

図２中の２系列生成部３３の処理手順の例を示す図。

【書類名】　図面

【図１】

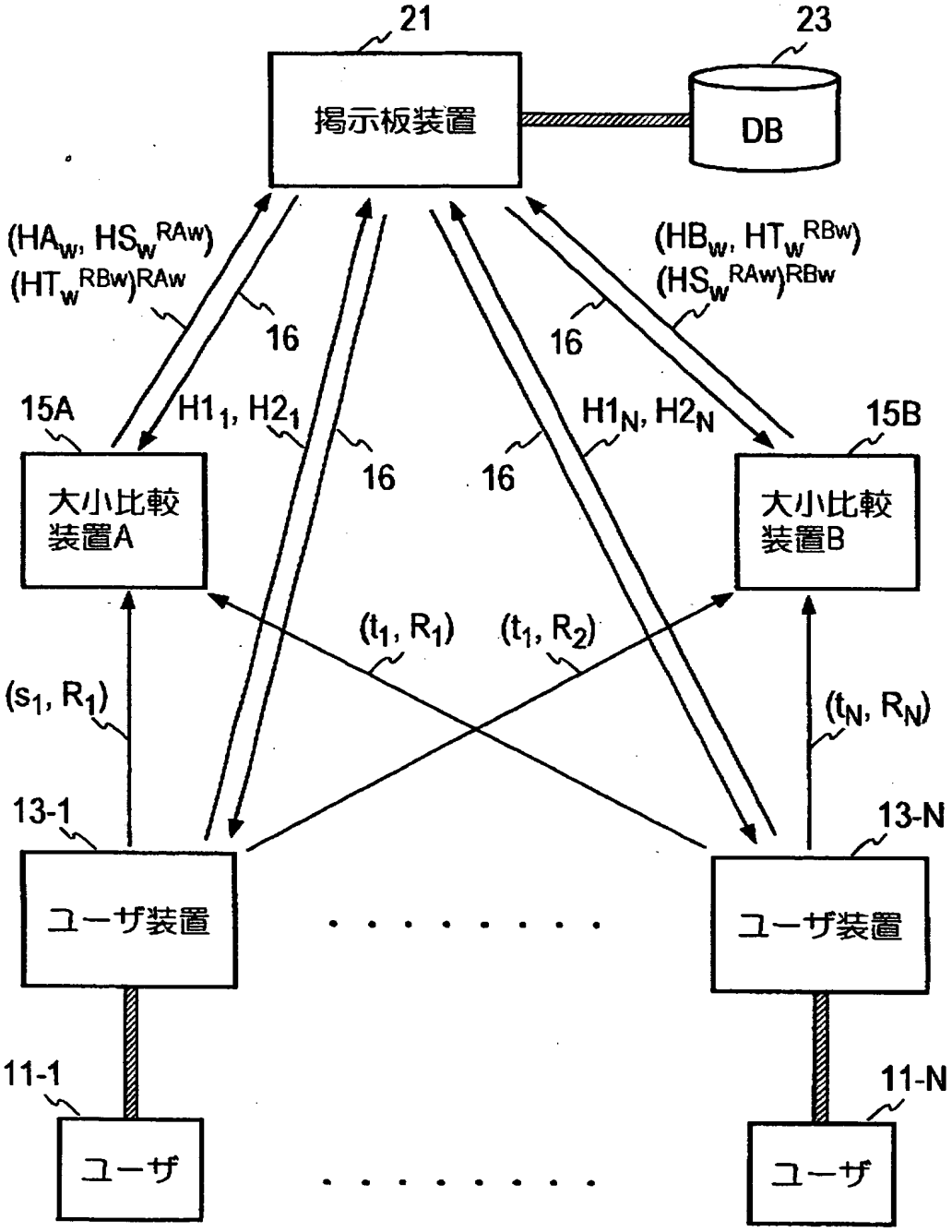
21
23
掲示板装置
DB
$(HA_w, HS_w^{RAw})$
$(HT_w^{RBw})^{RAw}$
16
$(HB_w, HT_w^{RBw})$
$(HS_w^{RAw})^{RBw}$
16
15A
$H1_1, H2_1$
16
16
$H1_N, H2_N$
15B
大小比較装置A
大小比較装置B
$(t_1, R_1)$
$(t_1, R_2)$
$(s_1, R_1)$
$(t_N, R_N)$
13-1
13-N
ユーザ装置
ユーザ装置
11-1
11-N
ユーザ
ユーザ

図1

【図２】

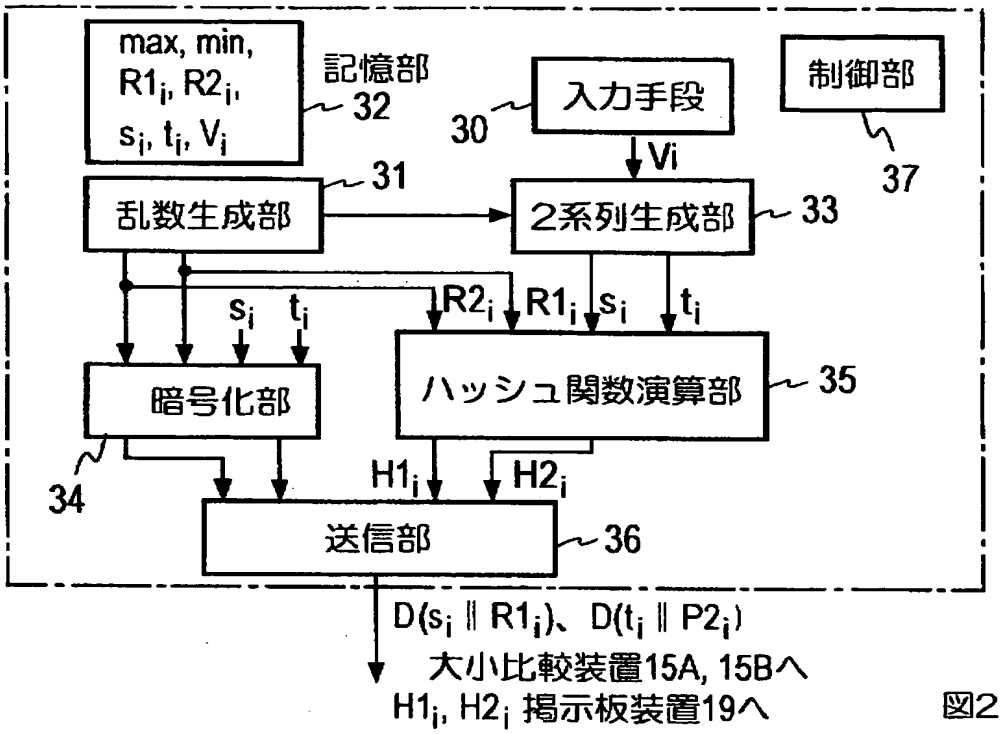
max, min,
$R1_i$, $R2_i$,
$s_i$, $t_i$, $V_i$
記憶部
32
入力手段
30
$V_i$
制御部
37
乱数生成部
31
2系列生成部
33
$s_i$ $t_i$
$R2_i$ $R1_i$ $s_i$ $t_i$
暗号化部
ハッシュ関数演算部
35
34
$H1_i$ $H2_i$
送信部
36
$D(s_i \| R1_i)$、$D(t_i \| P2_i)$
大小比較装置15A, 15Bへ
$H1_i$, $H2_i$ 掲示板装置19へ

図2

【図３】

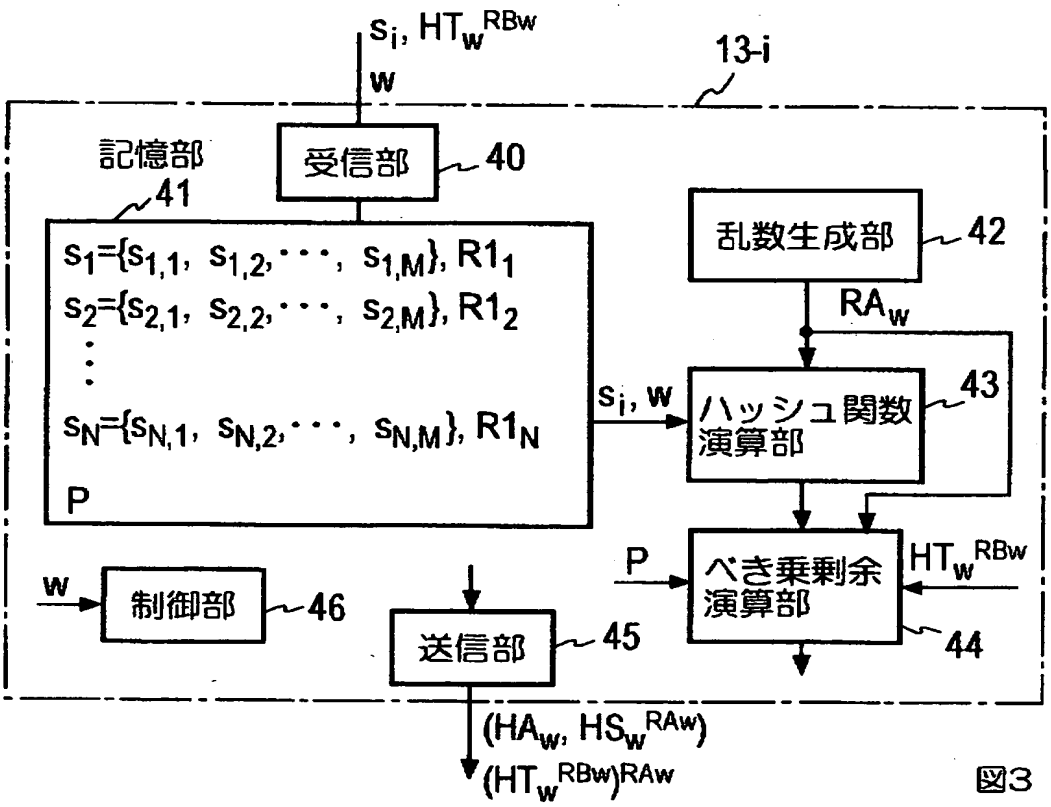
$s_i$, $HT_w^{RBw}$
w
13-i
記憶部
41
受信部
40
$s_1=\{s_{1,1}, s_{1,2}, \cdots, s_{1,M}\}$, $R1_1$
$s_2=\{s_{2,1}, s_{2,2}, \cdots, s_{2,M}\}$, $R1_2$
$s_N=\{s_{N,1}, s_{N,2}, \cdots, s_{N,M}\}$, $R1_N$
P
乱数生成部
42
$RA_w$
$s_i$, w
ハッシュ関数演算部
43
P
べき乗剰余演算部
$HT_w^{RBw}$
44
w
制御部
46
送信部
45
$(HA_w, HS_w^{RAw})$
$(HT_w^{RBw})^{RAw}$

図3

【図４】

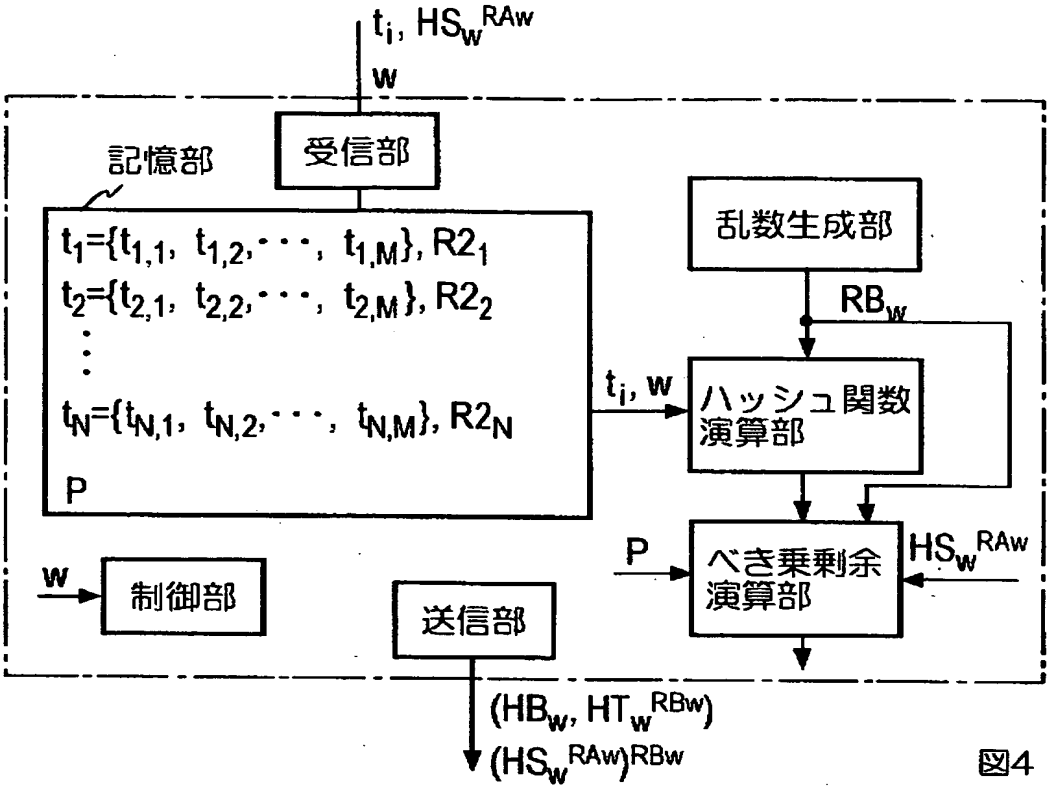
$t_i$, $HS_w^{RAw}$
w
受信部
記憶部
$t_1=\{t_{1,1}, t_{1,2}, \cdots, t_{1,M}\}, R2_1$
$t_2=\{t_{2,1}, t_{2,2}, \cdots, t_{2,M}\}, R2_2$
$t_N=\{t_{N,1}, t_{N,2}, \cdots, t_{N,M}\}, R2_N$
P
乱数生成部
$RB_w$
$t_i$, w
ハッシュ関数演算部
P
べき乗剰余演算部
$HS_w^{RAw}$
w
制御部
送信部
$(HB_w, HT_w^{RBw})$
$(HS_w^{RAw})^{RBw}$

図4

【図５】

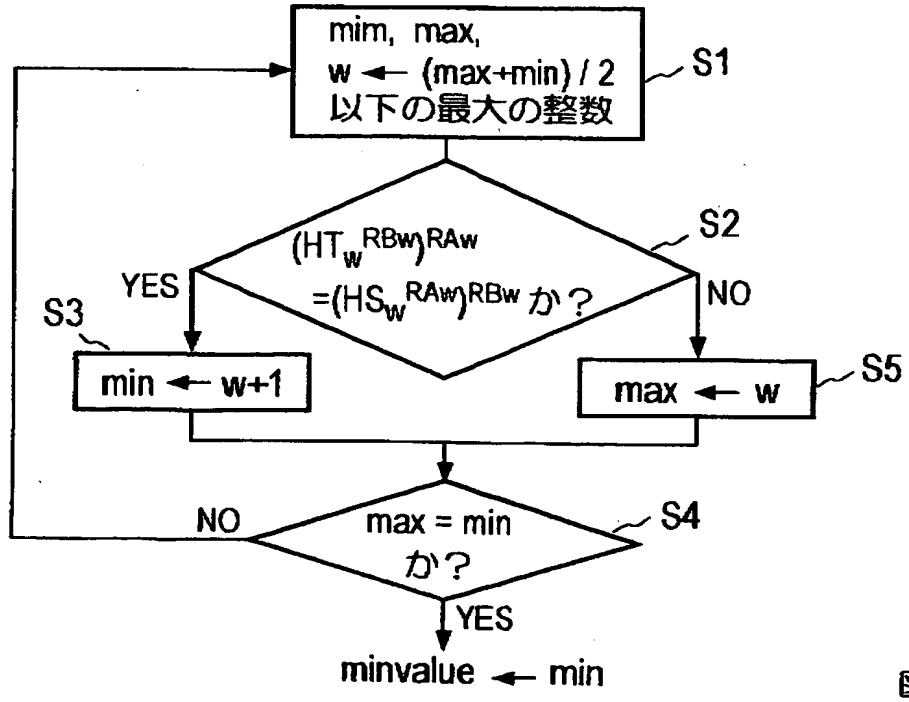
mim, max,
w ← (max+min) / 2
以下の最大の整数
S1
$(HT_w^{RBw})^{RAw}$
$=(HS_w^{RAw})^{RBw}$ か？
S2
YES
NO
S3
min ← w+1
max ← w
S5
NO
max = min
か？
S4
YES
minvalue ← min

図5

【図６】

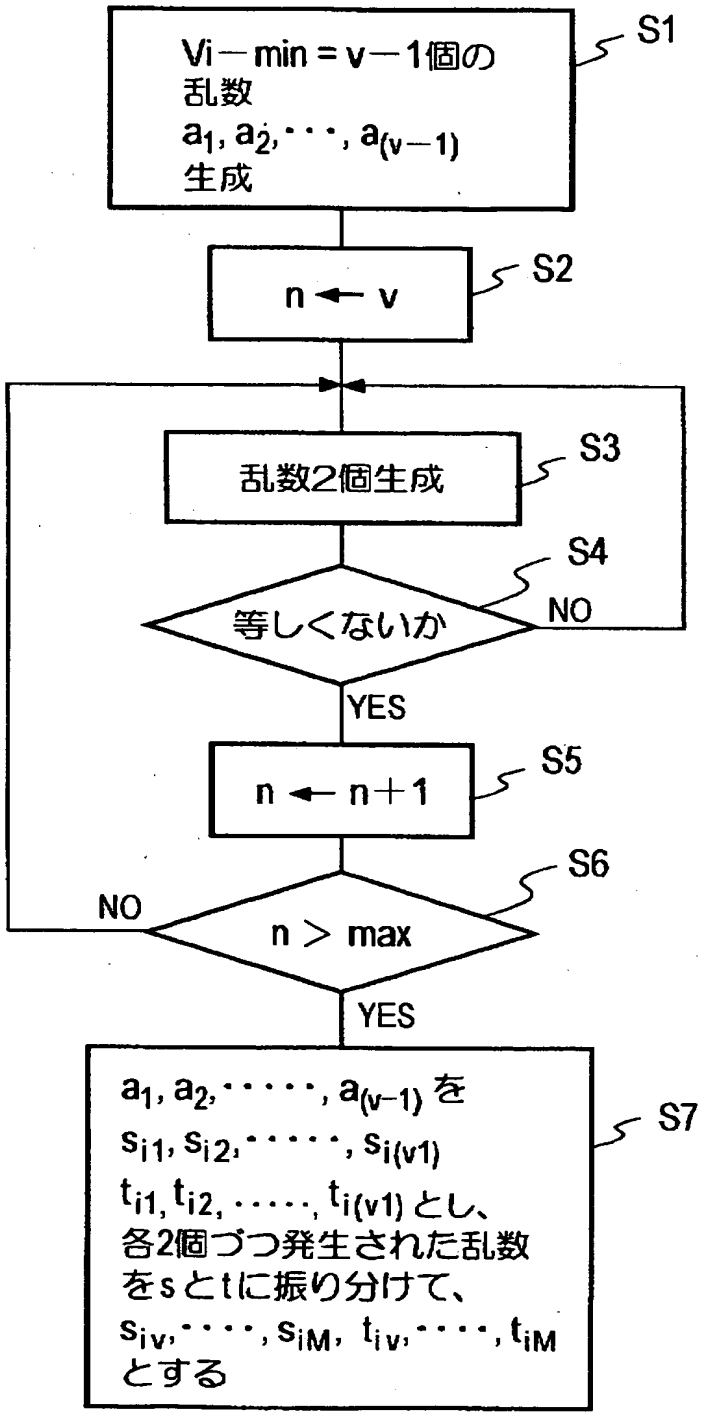
Vi－min＝v－1個の
乱数
$a_1, a_2, \cdots, a_{(v-1)}$
生成
S1
n ← v
S2
乱数2個生成
S3
等しくないか
S4
NO
YES
n ← n＋1
S5
n ＞ max
S6
NO
YES
$a_1, a_2, \cdots\cdots, a_{(v-1)}$ を
$s_{i1}, s_{i2}, \cdots\cdots, s_{i(v1)}$
$t_{i1}, t_{i2}, \cdots\cdots, t_{i(v1)}$ とし、
各2個づつ発生された乱数
をsとtに振り分けて、
$s_{iv}, \cdots\cdots, s_{iM}$, $t_{iv}, \cdots\cdots, t_{iM}$
とする
S7

図6

【書類名】　　要約書

【要約】

【課題】　競争入札に用いられ、ユーザは１回だけ入札値$V_i$を送る。

【解決手段】　入札最小値ｍｉｎから最大値ｍａｘまで各入札可能値に番号１，２，…,Ｍを付け、各ユーザｉは入札値$V_i$に対し、$s_i = \{s_{i1}, s_{i2}, \cdots, s_{iM}\}$ $t_i = \{t_{i1}, t_{i2}, \cdots, t_{iM}\}$、$s_{i1} = t_{i1}$, …, $s_{i,v-1} = t_{i,v-1}$, $s_{iv} \neq t_{iv}$, …, $s_{iM} \neq t_{iM}$なる２系列を作り（ｖは$V_i$の番号）、$s_i$と$t_i$を大小比較装置１５Ａと１５Ｂへそれぞれ秘密に送り、そのハッシュ値$H1_i = h(s_i)$, $H2_i = h(t_i)$を掲示板２１へ送り、大小比較装置１５Ａ，１５Ｂは番号ｗと対応して$s_1$～$s_N$から、各$s_{iw}$、$t_1$～$t_N$から各$t_{iw}$を取出し、Ｎ個の$s_{iw}$の連結$Seq_{s,w}$とＮ個の$t_{iw}$の連結$Seq_{t,w}$を作り、これらを一方向性関数を用いて、その各値を明すことなく比較し、等しければｗ以下の$V_i$はなく、異なっていればｗ以下の$V_i$があると判定し、ｗを変更して、最小値を決める。

【選択図】　　図１

# 出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社